(CLEAN COPY)

METHOD FOR CONTROLLING ACCESS TO A SENSITIVE AREA, PARTICUALRLY A TRANSPORT VEHICLE, BY BIOMETRIC VERIFICATION

CROSS REFERENCE TO RELATED APPLICATIONS

The present application is the National Stage of International Application No. PCT/FR03/00221, filed on January 23, 2003, which claims the benefit of French Application No. 02-00808, filed on January 23, 2003.

BACKGROUND OF THE INVENTION

[0001] The invention relates to access control to secure areas, particularly transport vehicles, and more particularly access control for boarding aircraft.

[0002] However, the invention is not limited to this particular transport application. It covers access control to all secure areas, for example such as access to secure rooms or parameters, secure companies, particularly banks, official organisations, particularly ministries, sports stadiums, etc.

[0003] And particularly in the context of accesses for boarding aircraft, it is particularly important nowadays to make sure that preliminary identity checks before boarding will not be bypassed.

[0004] In particular, it has become routine procedure to carry out several identity checks on the same person before allowing access onboard.

[0005] Thus, it is quite normal to check the passport of a person at the time that luggage is checked in, in other words when he is issued with his boarding card, and then to check the passport again when "reading at the boarding gate", in other words at the time of boarding, by

electronically reading the boarding card. The passenger is then obliged to board the aircraft.

[0006] This double check is expensive for airline companies.

SUMMARY OF THE INVENTION

[0007] The purpose of the invention is to satisfy a need for increasing the reliability and for reducing the costs of access controls made when boarding transport vehicles.

[0008] The invention achieves this purpose using a method of access control to a secure area, particularly to a transport vehicle, in which a person who would like to access the secure area is asked for personal data, these personal data are written on a card after they have been coded, this card is issued for the attention of this person and then at the time of access to the secure area, the personal data supplied by the person presenting this card are compared with the personal data written on the card to ensure that this person is actually the person authorised to use this card, characterised in that it includes two steps in which biometric readings are made directly on the person, one before the card is issued and the other at the access to the secure area, the recorded biometric data before the card is issued forming data written and coded on the card, the biometric data recorded at the access to this secure area being compared with the data on the card.

[0009] The invention also proposes an automatic access control module to a secure area, particularly a transport vehicle, comprising means of automatically reading data recorded on an access card to the secure area, characterised in that these read means are designed to

read biometric data registered on the card, and in that the module also comprises a sensor for sampling biometric data on a person and means of automatically comparing biometric data read on the card with data recorded by the sensor.

[0010] The invention also proposes a set of access control means to a secure area, particularly to a transport vehicle, comprising means of writing data onto cards controlling access to the secure area on a first site, and means of automatically reading these cards controlling access to the secure area on a second site, characterised in that the means on the first site also include a sensor for sampling biometric data on a person and means of writing these data on a card controlling access to the secure area, and in that the means on the second site comprise automatic means of reading biometric data written on the card, a sensor for sampling biometric data on a person, and means of making an automatic comparison between the biometric data read on the card and the data read by this sensor, these comparison means being designed to indicate if the data on the card and the data on the sensor belong to the same person.

[0011] Other characteristics, purposes and advantages of the invention will become clear after reading the detailed description given below with reference to the attached figure which shows an access control assembly according to a preferred variant of the invention.

DETAILED DESCRIPTION OF THE DRAWINGS

[0012] The following description is related to the special case of access control when boarding a transport means, particularly an aircraft. However, the invention is

not limited to this particular application. It includes access control to all secure areas, as mentioned above.

[0013] The means in Figure 1 are distributed in two modules, in other words a module 100 for printing the onboard access card and a module 200 for reading such a card at a boarding gate. This second module is normally called the "boarding gate reader".

[0014] The module 100 comprises mainly a printer 110 designed particularly to print boarding cards. An example of a boarding card is shown in Figure 1 as reference 300.

[0015] Apart from the fact that it includes means of printing text visible on such a card 300, this printer 110 has means of writing data on the card that are non-legible to the naked eye and that will be read by a machine. In this case, these means of writing data are memory means acting on a magnetic strip 310 on the card.

[0016] The module 100 also comprises an electronic fingerprint sensor 120. In the figure, this sensor is represented in the form of an independent housing 122 connected to the printer 110 through a wire link 130.

[0017] This housing 122 is provided with a secure area 125 in which one or more fingers are placed to record a fingerprint. Then, this type of record is sent by the sensor 120 to the printer 110 in the form of a digital file.

[0018] The printer 110 comprises a means of retranscribing the fingerprint data thus received onto the magnetic strip 310. A fingerprint is captured and recorded on the strip 310 in the form of a computer file.

[0019] The form of the reader module 200 at the boarding gate is similar to the module already described.

[0020] It also has a block 210 designed to interact with the magnetic strip 310 of the card 300, and a fingerprint sensor 220. This sensor 220 is integrated into the block 210 if possible, such that its secure area 225 is flush with the top surface of the block 210.

[0021] The objective of this module 200 is to acquire data written on the magnetic strip 310 of a card 300.

[0022] The module achieves this by including magnetic means for reading this strip 310.

[0023] This read module 200 also includes a processor in liaison with magnetic read means and with the fingerprint sensor 220. Therefore, the processor receives firstly fingerprint data read on the magnetic strip 310 of the card and secondly fingerprint data captured on a person by the sensor 220.

[0024] This processor then compares the two groups of data thus received in order to identify whether or not the fingerprint input by the sensor 220 and the fingerprint read on the card 300 are similar.

[0025] In an airport, these two modules 100 and 200 are preferably positioned as described below:

[0026] The module 100 is placed at a "check-in" desk, in other words a counter at which a passenger presents his ticket and luggage, if any, which are then transported towards the aircraft on a conveyor belt.

[0027] This type of check-in desk on which the module 100 is installed, is also the preferred location for an identity check before the card is printed.

[0028] The module 200 is placed at a final barrier before access to the aircraft, typically at the entrance to an aircraft access gateway.

[0029] By comparing the card carrier's fingerprint with the print recorded on the card, the second module 200 automatically checks that the card is used by the authorised person. This check is reliable, since it is based on electronic reading of fingerprints, which is technically very reliable.

[0030] The boarding card 300 contains data that are inevitably related to the person who already presented himself at the check-in desk, and his identity has been checked on his passport at the check-in desk.

[0031] Thus, if the person checks in at the check-in desk and is then substituted by another person who presents himself with the boarding card issued to the first person, this substitution will be detected immediately. Only the first person, and therefore the person whose identification has been verified, can use the card.

[0032] Therefore, it is no longer necessary to make a new identity check with reference to the passport when boarding, since the system automatically guarantees that the card carrier is the same person who checked in at the check-in desk. Therefore, a single identity check when the boarding card is printed is sufficient to ensure that the person boarding the plane has already provided his identity data, and has already been authorised.

[0033] Thus, with this access control system, the effects of the initial identity check continue until boarding, as a result of electronic tracking of the person by a ticket biometrically related to the person.

[0034] Furthermore with this system, the biometric data used may be recorded only on the card 300 and on no other computer medium, for example a database. Thus, the

passenger is assured that his fingerprint record is only kept on the flexible cardboard boarding card, that he can subsequently destroy.

[0035] Thus with this system, the extended use of biometric data for a passenger can be used, without contravening any regulations about keeping customer personal data.

[0036] More generally, the unpleasant aspect of taking a fingerprint, as is done when making a police record, is minimised by the guarantee that a person's fingerprints will not be kept.

[0037] The example embodiment described in this document is given as a preferred example.

[0038] However, there are other examples of embodiments of the invention that also have many advantages.

[0039] The example described above relates to a procedure for access to the secure area, including the step in which biometric data are written on the card, and also the effective use of this card, at the entry to the secure area.

[0040] In particular, in one procedure performed at the entry to the secure area, in which the card is written and used at the entry to the secure area, it is proposed to use a card other than a boarding card, for example a plastic card the same size as a credit card.

[0041] This type of cards is particularly advantageous due to the memory capacity of their magnetic strip. They are also advantageous when they contain a chip, also due to the chip storage capacity.

[0042] The card may perform other functions, such as an identity card or a "frequent flyer" type card, in other words a loyalty card incorporating a measurement of the

frequent use of the airline company made by the card carrier.

[0043] The card may also be used to enable access to other secure premises. The card can thus be an access card to company premises.

[0044] These various cards may be issued on entry to the secure area for the first time, in the step in which they are written. As a variant, the user supplies the card (for example a "frequent flyer" card) in which the biometric data input by the user are written close to the secure area, before being used for effective entry into the secure area.

[0045] The use of a magnetic record to write on the card as proposed in this description is not the only variant.

[0046] Thus, a biometric data record in the form of bar codes could be adopted rather than a record on a magnetic strip, or other means of entering biometric data that can be read by a machine could be used.

[0047] Preferably, data are written on the card so that a person cannot read them, and preferably they should be non-graphic, in other words so that a person cannot see the shapes, to avoid the possibility of fraud by graphic copy using a photocopier.

[0048] The invention has been described herein with reference to taking fingerprints. Other biometric records may be made using sensors, such as a record of parameters for the eye, and particularly the iris, and / or the person's voice recorded by a microphone and a sound analysis.

[0049] In another variant, the biometric data measured on the person consists of the geometry of the hand.

[0050] In yet another variant, the geometry of the face as captured by a camera is used as the biometric data, once again before the ticket is issued and then close to the aircraft.

[0051] According to another variant, the means of recording biometric data conform with the invention may be coupled to a database, to be input into this database.

557139_1.DOC